# Policy-based Approach for Secure Radio Software Download

Stango, Antonietta; Prasad, Neeli R.

*Published in:*
Proceedings of SDR'09 Technical Conference and Product Exposition

*Publication date:*
2009

*Document Version*
Publisher's PDF, also known as Version of record

# POLICY-BASED APPROACH FOR SECURE RADIO SOFTWARE DOWNLOAD

Antonietta Stango (Aalborg University, CTiF, Aalborg, Denmark, as@es.aau.dk)
Neeli R. Prasad (Aalborg University, CTiF, Aalborg, Denmark, np@es.aau.dk)

## ABSTRACT

The feature to be reconfigurable over the air interface is one of the main advantages of the SDR systems that offer operational benefit and considerable promises, but at the same time, introduces several important security issues like regulatory aspects, protection of contents, intellectual rights, and assurance of unaltered and appropriate software load. These aspects highlight that one of the main challenges in this field is the security of radio software download. The aim of this paper is to address the problem of secure radio software download in SDR devices, identifying existing solutions, comparison with regulations, and define a policy-based mechanism to secure download reconfiguration files into SDR devices according to regulations, needs of the service providers and users.

## 1. INTRODUCTION

A Software Defined Radio is defined [1] as a radio in which some or all of the physical layer functions are software controlled. The SDR technology responds to exponential growth to have a single device that can support a large numbers of wireless standards using a common platform. This provides an efficient solution to the problem of building multimode, multiband, multifunctional, wireless devices. The feature to be reconfigurable over the air interface is one of the main advantages of the SDR systems that hold considerable promise, introducing, at the same time, important security issues. Downloading software into terminals able to change the radio characteristics, introduces different security perspectives [2]:

- Regulatory -new software can change transmitter characteristics. The new hardware/software combination has to respect the appropriate regulations; it is very important that only approved, compatible software is installed.
- User -protection of content. The requirements in this case are authentication of the user and of the hardware with digital signatures, and authenticity/integrity of the new download by the user.
- Service provider -accounting for all billable time. The service providers can ask that the new software remain confidential to the users.
- Device manufacturer -assurance that the software load is appropriate for the target terminal and is unaltered.

These aspects highlight that one of the main challenges in this field is security of downloads, i.e. they must be signed and have digital authorization. Otherwise, downloads may be made to devices that could then broadcast on unauthorized bands, or to devices not compatible with the software, for example.
Security issues facing SDR technology include encryption, user identification, device authentication, and others; but the main issue is to secure the protocol of download reconfiguration files, which consists of secure the connection between the server and SDR device, mutual authentication, validation, data integrity, data encryption and decryption.
The scope of this work is to address the problem of secure radio software download in SDR devices, identify the existing solutions, compare them with regulations and define a policy-based mechanism to secure the download of reconfiguration files into SDR device, according to regulations and needs of service providers and users, considering that they are almost always connected and everywhere.

The remainder of the paper is organized as follows: in section 2 the motivations of this work on radio software download and the related work are described; section 3 is an overview of the regulatory aspects in Europe and in United States; in section 4 the proposed policy-based mechanism to download radio software and the download protocol are given; a security analysis has been done in section 5, and finally, conclusion and future work in section 6.

## 2. RADIO SOFTWARE DOWNLOAD

The motivation to work in the area of software download is mainly due to the need to upgrade wireless devices to provide additional capabilities and services, the need to correct software bugs or deficiencies in the existing software, and the need to roam with different air interface

standards. In these scenarios is clear that the most critical is the download of data or software able to modify configuration parameters, and this work will focus on this aspect.

Radio Software Download is defined as [3] "the process of delivering reconfiguration data and/or new executable code to a SDR device to modify its operation or performance". Radio configuration files (R-CFG) can include new parameters for modulation techniques, new power levels, and new operational frequencies. Following that, the term radio software download, used in this paper, is not to be confused with just any software download over the air interface, even if they have a lot of commonalities.
In general, a download process can be initiated by the server provider, the user, or an application. The radio software download process consists of three phases [2]:

- Pre-download, which includes service discovery, selection of security mechanisms, mutual authentication, authorization of the user, capability exchange, and finally the acceptance of the download.
- Download, that means physical transfer of the software, verification of the integrity, potential retransmission request, and placement in secure local storage.
- Post-download, which consists in installation, validation, non repudiation, reconfiguration of the SDR device.

### 2.1. Related Work

The issue of secure software downloads into a SDR device has been widely considered in literature from different points of view.
Brawerman et al. [4] proposed a protocol to secure the download of radio reconfiguration files in SDR. They propose a Lightweight version of SSL (LSSL) to secure the connection between the server and the SDR device and a protocol for securing the download of reconfiguration files. The protocol proposed works within a chosen subset of algorithms: X.509 certificate, used for authentication, LSSL or HTTP to establish a connection, and public/private key for validation.
In [5] the author proposes a policy-based authorization framework for software downloads to use in associations with SDR technologies, consisting of two policy model: within the trusted domain server and within the mobile device. Basically, the architecture proposed is based on the deployment of a security proxy server in every domain.
The problem of configuring mobile device over the air and a secure software download protocol in a trusted platform has been described in [6]. In [7] a threat analysis of a reconfigurable SDR device is done in order to address them with trusted computing functionality or to limit the level to which a threat can be exploited.
In [8] and [9] the software download is based on an approach where the server and the device share a secret key to provide data secrecy on the downloaded software. Digital signature is used to provide data authentication. Also the share-key scheme requires key management, which is not as scalable as the public key system.
Approaches for secure download of SDR software are described in [10], saying that specific of radio reconfiguration software are not the security mechanisms but the policy to be followed.
In [11], the authors focus on the protection aspect of software download and reconfiguration. In their scheme, X.509 certificates are embedded in the device to authenticate the software updates. The reconfiguration process is done in a secure environment, where both the hardware and software are assumed to be secure against all threats.
A model for assuring software downloads where software validation is performed in the network before the download has been proposed in [12], introducing an assurance agency responsible for performing software examination and validations.

In all these works, a number of different mechanisms to secure the download of software in SDR devices are proposed and described, with different approaches. What can be deducted is that, in literature there are already several means to protect the download and, in particular, the radio software.

## 3. REGULATORY ASPECTS

The radio software download is becoming an important topic for the regulatory organizations. Since this can affect the transmitting characteristics of the devices, it is very important that the combinations of hardware/software respect the rules and only software compatible is installed. Regulatory laws on SDR are relatively new, and vary depending upon geographical region; indeed are still under review.
Conventional regulatory restrictions on type-approval of radio devices will not allow industry to improve the capacities and consumers to extract the maximum benefit from SDR technologies. Recently the European Union [13] and the United States [14] extended regulatory considering the reconfigurability characteristics of SDR devices.

### 3.1. Regulatory Perspective in Europe

The European Parliament adopted, in March 1999, a Directive, defining new rules for the placing on the market and putting into service of Radio and Telecommunications

Terminal Equipment (R&TTE Directive 1999/5/EC) [13]. The scope was to promote a global and sustainable competitiveness of the Radio and Telecommunications Equipment Industries, ensuring safety, protection, and free movement of radio and telecommunications equipment in the EU. The Directive also promotes regulatory convergence and ensures research and innovation policies. The main changes to former regimes are:

- Introduction of manufacturers declaration of conformity;
- Obligation for network operators to publish their interfaces;
- Obligation for Member States to publish the rules to access the radio frequency spectrum;
- Obligation for Manufacturers to inform the end user of intended use and limitations of use.

Subsequently, a European committee, the Telecommunication Conformity Assessment and Market Surveillance Committee (TCAM), set up a group to discuss about the regulatory aspects of SDR with respect to the R&TTE Directive, which has defined [15]:

- SDR, a radio where essential radio parameters - normally subject to regulation - like frequency range, modulation type, maximum output power, etc. can be altered by changing software.
- Vertical market, all hardware and SDR software which is relevant for the declaration of conformity with the essential requirements for the intended use during the whole life cycle are controlled by one entity.
- Horizontal market, independent companies placing hardware and SDR software separately on the market, which when used together, are subject to the declaration of conformity with the essential requirements for the intended use of the equipment.

Further, they recognized that the responsibility for the product is a key issue and that an early collaboration between industry and regulators may assist in the minimization of the requirement for regulation.

### 3.2. Regulatory Perspective in the United States

In the US the FCC (Federal Communications Commission) released, in March 2005, a set of rules outlining an alternative method for certification of devices whose radio frequency and power characteristics can be modified by software (Software Defined Radio devices). The rules allow manufacturers, who have certified under the new process, to update the software on the devices without re-certifying the devices with the FCC [14]. The FCC allows also the use of Free and Open Source Software (FOSS) on SDR devices, but with the belief that building security measures to protect the software against modification would create a "high burden" during the certification process to demonstrate that it is sufficiently secure. The FCC's rules allow FOSS developers not affiliated with device manufacturers to continue work on their software without restriction. They allow SDR manufacturers to employ FOSS for most of the functionality of their devices and they leave open the possibility that a device using a purely FOSS-based software platform could also pass FCC certification if it managed to demonstrate the soundness of its security strategy.

The regulatory agencies are improving the rules from the point of view of SDR devices, but nevertheless, further reform, especially in the area of spectrum policy, will be necessary before the maximum benefits from SDR can be realized.

It is clear from this short analysis that the radio software download and the following reconfiguration have to respect the legislation in operation in the country where the device is used.

## 4. PROPOSED SECURE RADIO POLICY-BASED SOFTWARE DOWNLOAD

Securing radio software download for SDR devices is an issue that includes several aspects as described in previous sections. Analyzing the state of the art highlights that to handle the security services there are already different ways, like encryption, authentication, non-repudiation, so developing new security mechanisms is challenging and not always secure [10]. The main issues that have been identified are the establishment of a secure connection between the source of the radio software and the SDR device, and, further, considering that the most used mechanism to protect software download is sign content, the design of an underlying policy to determine the entity that can certify the parties involved.

### 4.1. Proposed Policy-Based Model

A security policy is a plan or course of action for tackling security issues made by an authority, thus a security policy becomes a set of regulations. In the specific case of SDR, a security policy is defined as [16] "a set of permitted operating states and state transitions. The SDR security policy may also contain rules regarding authentication mechanisms events to be audited, and actions to be taken in response to an event." To analyze the radio software download the scenario depicted in Figure 1 has been considered. The SDR devices are connected to a Reconfiguration Server (that can be connected with a database or storage area network, not showed in figure) through a wireless network. In the figure the server is connected with the manufacturer and with the network

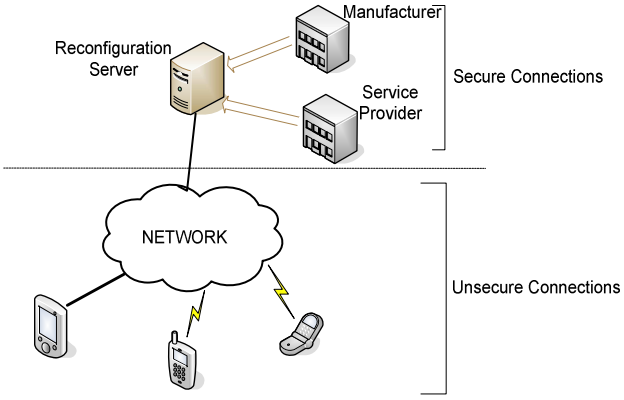


**Figure 1. Radio software download scenario**

operator; in general it can be connected with every entity that can be a Source of Reconfiguration (SoR) files. The following assumptions have been made:

- The connections between the server, the SoR (and the storage) can be considered trusted.
- The access network and the SDR devices are susceptible to attacks.
- The Reconfiguration Server (RS) is a Trust Third Party (TTP) able to take policy-based decisions.

In this scenario, downloads of reconfiguration files can be requested by users or provided by the RS on request of manufacturers/network operators.

The entities involved in the management of the policies in this scenario are divided between the RS and the SDR device. In the model proposed, the RS has the role of a Trusted Third Party (TTP) responsible for deciding the type of connection that has to be established for the communication and for the download, what needs to be signed, sign it if necessary, and to validate the content of the software download [12] according with the security policy. For example the security requirements of the Regulation Authority (RA), ensure that the device will not cause interference or function out of its defined spectrum, with the software producer or manufacturer, protecting any intellectual rights, and considering the privacy rights of the users.

In Figure 2 is shown the policy manager in the RS. The RS is in charge of verifying that the reconfiguration software provided is respecting the regulations of the RA, that the users downloading that software are respecting the rights of the SoR (intellectual rights, billable services), that the privacy of users is safeguarded (meaning that personal data are not disclosed if not necessary), and the validity of the software. The policy manager is also responsible for providing storage for received policies profiles (policy database in the figure) coming from RA and SoR.

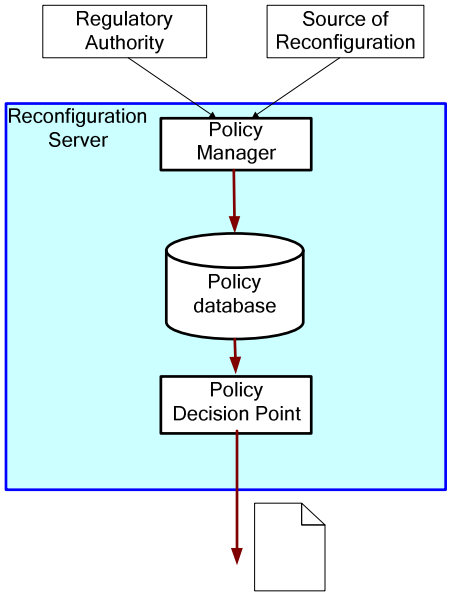


**Figure 2. Policy components in the Reconfiguration Server**

Furthermore, the RS, being aware of the SoR (i.e. if it can be considered trusted and the level of trust), is able to take decisions in the Policy Decision Point, on the type of connection that must be established, on who is authorized to sign the contents of download, and what kind of meta information should be included in the certificate.

The Policy Decision Point is responsible for parsing and validating the policies, which are communicated to the SDR device in form of a meta-description.

In Figure 3, the policy components presented in the SDR device are depicted. The meta-information received from the RS are extracted in the Policy Decision Point to verify that they can be fulfilled. The role of this decision point is to approve or deny the download based on the information coming from the Policy Enforcer, which is checking the characteristics of the device (if it is conforming to the new configuration), considering its status, i.e. if it really needs reconfiguration (version of the software or parameters), and validates the digital signatures. When the download has been approved the Policy Decision point in SDR device supplies all the requirements coming from the policy to the Device Manager, which provides the communication interface and performs the download/installation of the reconfiguration files.

### 4.2. Protocol Description

The radio software download protocol can be summarized in the following steps:

1. Request of download. The request can be done by users or provided by the RS on request of manufacturers/network operators.

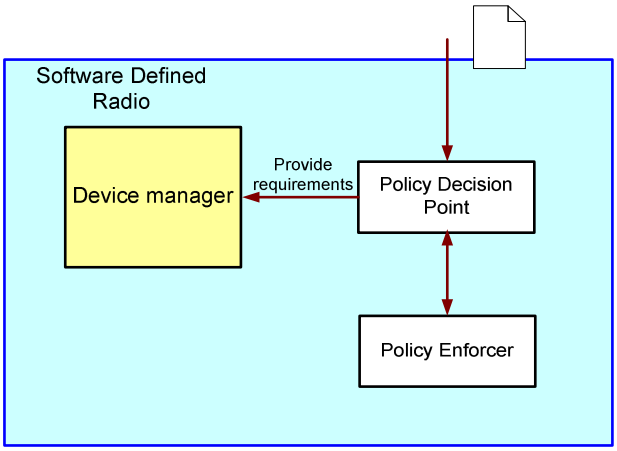


**Figure 3. Policy components in the SDR device**

2. Mutual authentication between SDR device and RS.
3. The RS establishes the policy for download, meaning the type of connection, the entity that is going to sign the contents, the constraints to respect the regulations, and validation of software.
4. Establishing a connection between SDR device and RS, depending on the presence of proprietary information in the radio software download (SSL or HTTP).
5. Sign contents, if necessary, and exchange of meta-information for policy and certificates.
6. Download of software.
7. Installation and storage of software by the Device Manager.

After the download and the installation, an encrypted copy of the radio software can be stored in the SDR device for future use, but before to be reactivated the Policy Decision Point in the SDR device has to check that there are no restrictions. This means to verify the policy on the software, coming from the RS, and the policy applied to the device.
The policy-based approach, presented in this work, allows existent security mechanisms to be used, however which mechanism, and which is the entity signing the certificates, will be selected in the RS, based on the policy. In this way, there is no need for interaction with the user, reducing a lot the risks of security attacks. Further, the RS being able to validate the software, based on the level of trust of the sources, makes real the possibility to download software from open sources and not only from specific providers.

## 5. SECURITY ANALYSIS

The security analysis includes the confidentiality, integrity protection of the data in the transmission, and the prevention of unauthorized access to the application during execution and while in storage.
The transmissions of data from a SoR to the RS are supposed to be in a secure environment.
The solution proposed provides secure transmission from the RS and SDR device, since the confidentiality and integrity of the software are protected by mutual authentication and content signed.
Using mutual authentication to send messages, a connection is possible only if the client trusts the server's certificate and the server trusts the client's certificate. In our case, mutual authentication ensures, not only that the person behind the SDR device is who he claims to be, but also proves that the server, he is communicating with, is who it claims to be, protecting the confidentiality of sensitive information by ensuring that the RS is genuine. Mutual authentication also helps to protect users from masquerade attacks that lead to transaction fraud and assures the access control to the RS.
The integrity of the data is assured by the RS which sign the contents. The digital signature ensures by hash functions that the software has not been modified (integrity) and attests its SoR (authentication of the origin). If the provider is not certified (meaning that is not the manufacturer or service provider) it is task of the RS validate and certify the origin of data.
Radio software can also be stored in the SDR device because the same mechanisms that protect the software in transit from the RS can protect it for future use.

## 6. CONCLUSIONS AND FUTURE WORKS

This work proposes a policy-based mechanism to secure the download of reconfiguration files into SDR devices, according to the regulations, and the needs of the service provider and user. The proposed mechanism is based on a Reconfiguration Server, which is a TTP able to make decisions about the policy to use for the download as well as decide which entities (itself or manufacturer or service provider) have to sign the content of the download. The policy can vary with the regulatory rules, with the SoR, with the content, and also with the market (vertical or horizontal). Moreover, the RS has the task of validating software that is not originating from an official source, in this way software also coming from an open source can be used for saving resources in the device.

The future work will be the development of a policy language with a set of policy classes and instances and the improvement of the protocol for download, mainly defining and implementing the mutual authentication algorithm and providing a trust mechanism from the RS and open sources entities for download.

## 7. ACKNOWLEDGMENT

The work in this paper is part of the Danish project SUBWAY (Secure SDR-enabled wireless networks ability) founded by CSDR (Center for Software Defined Radio).

## 8. REFERENCES

[1] Software Defined Radio Forum, "SDRF Cognitive Radio Definitions", SDRF-06-R-0011-V1.0.0, November 2007.

[2] Software Defined Radio Forum, "Requirements for Radio Software Download for RF Reconfiguration", SDRF-02-A-007-v1.0.0, Feb. 2002.

[3] Software Defined Radio Forum, "Overview and Definition of Software Download for RF Reconfiguration", SDRF-2002-A2, Aug. 2002.

[4] A. Brawerman, D. Blough and B. Bing, "Securing the Download of Radio Configuration Files for Software Defined Radio Devices", Proc. of the ACM international Workshop on Mobility Management and Wireless Access, October 2004.

[5] E. Gallery, "A Policy-Based Framework for the Authorisation of Software Downloads in a Mobile Environment", In 2nd Software Defined Radio Technical Conference (SDR03), Orlando, Florida, November 2003.

[6] E. Gallery, A. Tomlinson, "Protection of Downloadable Software on SDR Devices", Software Defined Radio Technical Conference SDR05, November 2005.

[7] E. M. Gallery, C. J. Mitchell, "Trusted computing technologies and their use in the provision of high assurance SDR platform"', Software Defined Radio Technical Conference, Orlando, Florida, November 2006.

[8] L. B. Michael, M. J. Mihaljevic, S. Haruyama, R. Kohno, "A Framework for Secure Download for Software Defined Radio", IEEE Communications Magazine, Volume: 40, Issue: 7, Page: 88-96, July 2002.

[9] L. B. Michael, M. J. Mihaljevic, S. Haruyama, and R. Kohno, "A proposal of architectural elements for implementing secure software download service in software defined radio", 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, 2002.

[10] R. Falk. M. Dillinger, "Approaches for Secure SDR Software Download," SDR Forum Tech. Conf., Phoenix, AZ, Nov. 2004.

[11] R. Falk, F. Haettel, R. Atukula, U. Lücking, "Protecting Reconfiguration in Future Mobile Communication Systems", Database and Expert Systems Applications, Sixteenth International Workshop, August 2005.

[12] S. Sabetghadam, M. Niamanesh, J. Esmaeili, "A Model for Sured Software download on mobile Terminals", International Conference on Communications and Mobile Computing, January 2009.

[13] http://www.rtte.org/

[14] Software Freedom Law Center, "FCC Rules on FOSS and Software-Defined Radio", 6 July 2007.

[15] D. Bourse, K. El-Khazen, K. Moessner, D. Grandblaise, "End-to-End Reconfigurable Systems: The E2R Responsibility Chain Concept", SDRF Technical Conference, Anaheim, USA, November 2005.

[16] Software Defined Radio Forum Security Working Group, "High-Level SDR Security Requirements", document SDRF-06-A-0002-V0.00, 19 January 2006.